Security Work Group
http://www.nitc.state.ne.us/tp/workgroups/security/index.htm

Monday February 9, 2004
10:00 A.M. to Noon
Executive Building Basement Conference Room
521 South 14th Street
Lincoln, Nebraska

Minutes

Participants

Ryan	Booton	Dept. of Banking
Beverlee	Bornemeier	IMServices
Randy	Cecrle	Workers Compensation Court
Steve	Cherep	Health and Human Services System
Cathy	Danahy	Secretary of State / Records Management
Rex	Gittins	Dept of Natural Resources
Rob	Grower	Dept. of Natural Resources
Steve	Hartman	IMServices
Steve	Henderson	IMServices
Jerry	Hielen	IMServices
Steve	Mayer	Health and Human Services System
Zac	Reimer	UNL
Leona	Roach	University of Nebraska
Steve	Schafer	Nebraska CIO
Bob	Thompson	Dept. of Roads
Dan	Ward	Division of Communications
Brad	Weakly	IMServices

A. Vulnerability Testing
   1. January internal vulnerability scan. Brad Weakly (IMS) described recent activity by IMS and DOC to inventory the ports and services that are exposed to the inside of the state's network. They are working to create automated scans with a scheduling capability that would be available for agencies to use. Results would be posted to a protected web site that would available to agencies. IMS and DOC are seeing the same types of ports and services openly available that Omni Tech suggested should be turned off. Although firewall configurations may protect these services from external access, they pose a potential exposure to viruses or other risks within the network.
   2. Follow-up of External Intrusion Security Assessment. Steve Schafer explained that he was working with Omni Tech to conduct a repeat of Phase II – vulnerability scan of the state's network. The timeframe would be mid or late March. Discussion indicated that the scope of services should include:
      a. An on-site visit;
      b. Comparison with the previous scan;
      c. Reporting in the same format as before.

3. Review SAN Top 20 List. Steve Schafer referred to this list as a good benchmark to follow. Any agency that has protected itself against the SAN Top 20 should fare well in any vulnerability assessment.

B. Layered Security. Dan Ward and Brad Weakly discussed their approach to layered security. There are separate firewalls protecting static IP addresses (about 200 servers), dynamic IP addresses (about 10,000 plus users), and 164.119 addresses (relatively few servers and users). The firewalls for the static IP addresses and dynamic IP address are effective because they include specific rules and known devices. The firewall for the 164.119 addresses has few rules. For the past year, DOC and IMS have been trying to move all 164.119 addresses to one of the other firewalls. This has not been successful, because there are some circumstances that make it difficult to change to a different IP address, and it has been impossible to determine the exact ownership and location of many 164.119 addresses. Instead, DOC/IMS plans to configure a firewall that segregates 164.119 traffic from the rest of the state's network.

   Steve Schafer asked about the feasibility of an IP registration system and offered to send a letter to agencies asking them to identify what 164.119 addresses they own. This information will be needed for the Omni Tech vulnerability scan.

C. Minimum Standards for Network Security
   Discussion centered on what additional steps should be taken to improve security of the state's network. Suggestions included:
   - Develop a security architecture that provides an ability to isolate sections of the network and allows for quick recovery;
   - Include server protection;
   - Include desktop security;
   - Provide a central repository for security patches;
   - Provide training and technical assistance on installing security patches;
   - Explore utility service concept for virus protection, patch management, and network management, especially for small agencies;

   There is also a need for education of employees – both technical staff and end users. End users need to be aware of security concerns, including security for home computers that could be sources of vulnerability to the state's network. A regular feature on computer security in the Statehouse Observer is one idea. Technical staff would benefit from workshops on topics such as hardening servers.

D. Central Notification of Security Threats
   Time did not allow for much discussion, but the consensus was to continue distribution of the security notices from the multi-state ISAC (issued by the New York State Office of Cyber Security) and other sources. Steve Schafer expressed a desire to shift this responsibility to an operational entity, but will continue serving this function for now.

E. Other Security Initiatives

Steve Hartman described the progress on the directory services project, which will provide a central system for authentication. The Nebraska Directory Services project is rapidly approaching implementation of the Enterprise Directory and Portal. A series of stress tests and DRP/failover tests are scheduled for the middle of February. A small pilot group of users will be testing the Portal for accuracy, usability, and Section 508 compliance. Once these tests have been completed, IMServices will start rolling out the Portal and the Enterprise Directory. Some of the accomplishments to date are:

1. Connecting the NIS for pulling all State staff info into the Directory
2. Limited synchronization with Active Directory
3. Agency Portal pages (templates) developed
4. Granular role-based authorization
5. Role-based Administrative console

Steve Schafer gave an update on disaster recovery and business continuity planning. Using a grant from NEMA, DAS has issued an RFP for selecting a contractor to provide Business Continuity Consultation Services. Initially, this will focus on business continuity for core DAS functions that support other agencies. The RFP will provide a methodology and pricing that other agencies can use, if additional grant funds become available.

F. Future Topics:

1. HHSS will report on their procedures for virus and patch management.
2. HHSS will report on their procedures for controlling remote devices.
3. IMS and DOC will document the network architecture and provide an update on implementation.
4. IMS will present draft revisions to the network security standards. The revisions will address containment policies and procedures and address additional topics such as desktop security.
5. The agenda will include time to develop a plan for holding workshops and providing other education strategies.

G. Next Meeting Date – Monday April 12, 2004. Location: NSOB LLC. (NOTE: April 12 meeting was canceled.)